SECTION I—CLAIMS

Amendment to the Claims:

This listing of the claims will replace all prior versions and listings of claims in the application. Claims 1, 14, and 18-19 are amended herein. Claims 17 and 20 remain canceled without prejudice. New claims 24-25 are presented herein. Claims 1-16, 18-19, and 21-25 remain pending in the application.

Listing of Claims:

1. (Currently amended) A method comprising:

intercepting a request for a web page from a user device, the user device connected with a blocked port of a packet forwarding device, the blocked port preventing the user device from accessing a network coupled [[to]] with the forwarding device;

directing the user device to a network login page for authentication;

executing an authentication routine ~~attempting~~ to authenticate the user device based on input received at the network login page;

sending an unblock port command to unblock the blocked port, when the authentication routine ~~attempting to authenticate the user device based on input received at the network login page~~ results in a positive authentication response for the user device; and

allowing the user device to access the network when the blocked port is unblocked.

2. (Previously presented) The method of claim 1, wherein intercepting a request from the user device comprises intercepting a HyperText Transfer Protocol (HTTP) request from the user device.

3. (Original) The method of claim 2, further comprising receiving a Domain Name Service (DNS) request to translate a domain name specified in the HTTP request into an Internet Protocol (IP) address.

4. (Original) The method of claim 3, further comprising proxying the DNS request to a DNS server.

5. (Original) The method of claim 4, further comprising receiving a response from the DNS server with a DNS-resolved IP address.

6. (Previously presented) The method of claim 5, further comprising sending the DNS-resolved IP address to the user device.

7. (Previously presented) The method of claim 6, further comprising intercepting a request from the user device directed to the DNS-resolved IP address.

8. (Previously presented) The method of claim 7, wherein directing the user device to a network login page for authentication comprises responding to the user device with a redirect to a Uniform Resource Locator (URL) address for the network login page.

9. (Previously presented) The method of claim 8, further comprising receiving a DNS request from the user device to translate a domain name for the network login page into an IP address.

10. (Previously presented) The method of claim 9, further comprising responding to the user device with the IP address of the packet forwarding device.

11. (Previously presented) The method of claim 10, further comprising receiving from the user device, a request to the IP address of the packet forwarding device.

12. (Previously presented) The method of claim 11, further comprising responding to the user device with the network login page.

13. (Previously presented) The method of claim 1, further comprising receiving an authentication request from the user device via the network login page, the authentication request comprising user identification data.

14. (Currently amended) The method of claim 13, wherein executing the authentication routine ~~attempting~~ to authenticate the user device based on input received at the network login page comprises parsing the authentication request and forwarding the authentication request to an authentication server.

15. (Previously presented) The method of claim 14, wherein parsing the authentication request and forwarding the authentication request to the authentication server comprises creating a packet with the user identification data in accordance with the RADIUS communications protocol and forwarding the RADIUS packet to a RADIUS server.

16. (Original) The method of claim 15, further comprising receiving a response from the RADIUS server to indicate whether the user identification data is authentic.

17. (Canceled).

18. (Currently amended) An apparatus comprising:

a packet forwarding device coupled with a network, the packet forwarding device having a blocked port, the blocked port to prevent a user device connected with the blocked port from accessing the network until the user device is authenticated; and

an authenticator discovery controller coupled with the packet forwarding device, the authenticator discovery controller to:

intercept a request for a web page from the user device,

direct the user device to a network login page for authentication,

execute an authentication routine ~~attempt~~ to authenticate the user device based on input

received at the network login page, and

send an unblock port command to unblock the blocked port, when the authentication routine ~~attempt to authenticate the user device based on input received at the network login page~~ results in a positive authentication response for the user device.

19. (Currently amended) The apparatus of claim 18, wherein the authentication routine ~~attempt~~ to authenticate the user device based on the input received at the network login page comprises sending the input received to a network login controller coupled with the packet forwarding device to ~~attempt to~~ authenticate the user device based on the input received ~~at the network login page~~ and send the positive authentication response to the authenticator discovery controller when the user device is successfully authenticated.

20. (Canceled).

21. (Previously presented) The apparatus of claim 19, wherein the unblock port command to unblock the blocked port originates at the network login controller.

22. (Previously presented) The apparatus of claim 21, wherein the authenticator discovery controller to further:

receive a Domain Name Service (DNS) request from the user device, and

proxy the DNS request to a DNS server to translate a domain name into an Internet Protocol (IP) address.

23. (Original) The apparatus of claim 18, wherein the packet forwarding device is a switch.

24. (New) The method of claim 1, wherein the blocked port comprises a default state, the default state characterized as operating in a non-forwarding, un-authorized, and blocked functionality mode.

25. (New) The method of claim 24, wherein the blocked port returns to the default state after one or more events including:

a pre-determined period of inactivity by the authenticated user device is exceeded;

a reset signal is received from a network login controller;

an administrator forces the blocked port back to its default state;

a network connection associated with the authenticated user device is disconnected; and

a user of the authenticated user device logs off of the authenticated user device.